

UNITED STATES DISTRICT COURT

for the

Eastern District of Pennsylvania

In the Matter of the Seizure of  
(Briefly describe the property to be seized)

The Internet Domain Name "renopharma.com"

Case No. 17-M- 1276

APPLICATION FOR A WARRANT  
TO SEIZE PROPERTY SUBJECT TO FORFEITURE

I, a federal law enforcement officer or attorney for the government, request a seizure warrant and state under penalty of perjury that I have reason to believe that the following property in the EASTERN District of VIRGINIA is subject to forfeiture to the United States of America under            U.S.C. §            (describe the property):

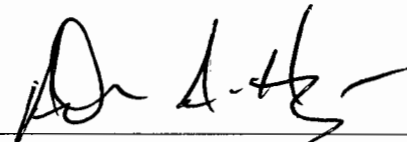
18 U.S.C. §§ 981(b), 1834, 2323, and 21 U.S.C. § 853(f),  
for violations of 18 U.S.C. § 1832 (theft of trade secrets).

THE FOLLOWING PROPERTY: The internet domain name remopharma.com which is registered to Yu Xue, via registrar Verisign, Inc.

The application is based on these facts:

See Affidavit of Special Agent ANDREW HAUGEN Attached.

☐ Continued on the attached sheet.



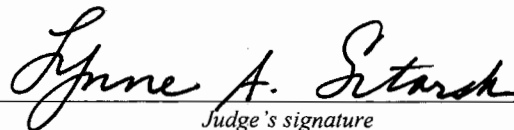
Applicant's signature

SPECIAL AGENT ANDREW HAUGEN

Printed name and title

Sworn to before me and signed in my presence.

Date: September 19, 2017



Judge's signature

City and state: PHILADELPHIA, PENNSYLVANIA

HON. LYNNE A. SITARSKI U.S. MAGISTRATE JUDGE

Printed name and title

**AFFIDAVIT IN SUPPORT OF APPLICATION FOR ARREST WARRANT**

I, Andrew Haugen, Special Agent with the Federal Bureau of Investigation (FBI) being duly sworn, do hereby depose and state as follows:

**I. INTRODUCTION**

1. I am a Special Agent (S/A) with the Federal Bureau of Investigation (FBI). I have been a Special Agent since July 2010. Prior to that, I was an analyst employed by the FBI, assigned to the International Operations Division where I worked fugitive matters through INTERPOL.

2. I have experience investigating violations of federal law, to include theft of trade secrets, wire fraud, and money laundering, among other violations. Although I am currently assigned to a public corruption squad, I was previously assigned to the Counterintelligence Squad. As a federal agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

3. The statements contained in this affidavit are based on my own knowledge and on information provided to me by other law enforcement officers. Because this affidavit is being submitted for the limited purpose of securing a seizure warrant, I have not included each and every fact known to me concerning this investigation, but rather those facts which I believe are necessary to establish probable cause.

4. In addition, some of the e-mails referenced below were written in whole or in part in Mandarin Chinese. I do not read Mandarin Chinese. Therefore, I am relying upon summaries of these e-mails provided to me by Mandarin speaking FBI agents, linguists, and contractors. Finally, I reference a number of seized e-mails in this affidavit. I note that there are discrepancies in the date and time stamp of some of the e-mail communications based on a variety of factors to include location of sender/recipient and the location of the email service provider servers, and the e-mail service providers use of particular time zones. Thus, the same e-mail seized from different accounts may have different time stamps.

**II. PURPOSE OF WARRANT**

5. I submit this affidavit in support of a warrant to seize the following domain name which is being used to facilitate the offense conduct described below (the **SUBJECT ACCOUNT**): **renopharma.com**, which is registered with VeriSign, Inc., which has its headquarters at 21355 Ridgetop Circle, Dulles, Virginia. The procedures by which the government will seize the **SUBJECT ACCOUNT** are described in "Attachment A" to this affidavit.

6. As described in more detail below, the FBI currently is investigating the creators of the **SUBJECT ACCOUNT**, namely YU XUE, TAO LI, YAN MEI, and TIAN XUE, for violations of Title 18, United States Code, Sections 1343 (wire fraud), 1832 (theft of trade secrets), and 1956 (money laundering).

7. In connection with the investigation, on January 20, 2016, a grand jury in the Eastern District of Pennsylvania returned a 43-count indictment charging YU XUE, TAO LI, YAN MEI, and TIAN XUE with the offenses described above and conspiracy to commit these offenses. As described in detail below, the **SUBJECT ACCOUNT** was property used and intended to be used to commit or facilitate the commission of the violations of 18 U.S.C. Section 1832, and, therefore, is subject to forfeiture to the United States pursuant to 18 U.S.C. Sections 1834 and 2323. The government seeks to seize the **SUBJECT ACCOUNT** pursuant to 18 U.S.C. Sections 981(b), 1834, and 2323, and 21 U.S.C. Section 853(f).

### **III. BACKGROUND**

#### **A. In General**

8. In summary, the subjects of this investigation stole very valuable trade secret and other confidential information from GlaxoSmithKline (“GSK”) for their own pecuniary benefit. YU XUE and LUCY XI are former GSK employees. The stolen information contains the blueprints to manufacture cutting-edge pharmaceutical products currently being developed by GSK and other important GSK research information. This data potentially could be sold for millions of dollars to rival pharmaceutical companies, and it would also be useful information for a start-up pharmaceutical company. The management of GSK is aware of this investigation and, to the best of my knowledge and belief, has been fully cooperative with this investigation to date.

9. To facilitate the offenses, the conspirators established three corporations – Renopharma, Inc., Nanjing Renopharma, Ltd, and Shanghai Renopharma, Ltd. (collectively referred to herein as “RENOPHARMA”). These corporations operated to market and sell the stolen data to GSK’s competitors in China.

10. Also, to facilitate the marketing and sale of the stolen GSK intellectual property, the defendants created a website for RENOPHARMA, called “**renopharma.com**” (the **SUBJECT ACCOUNT**), through GoDaddy.com, LLC. The **SUBJECT ACCOUNT** advertises the sale of RENOPHARMA services and products, and, as described in more detail below, these services and products were stolen from GSK. As described below, the **SUBJECT ACCOUNT** was temporarily disabled by the service provider in May 2017 at the request of the FBI pending application of this seizure warrant.

#### **B. Technical Background**

11. Based on my training and experience and information learned from others, I am familiar with the following terms:

a. Internet Protocol Address: An Internet Protocol address (IP address) is a unique numeric address used by computers on the Internet. An IP Address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. An IP address acts much like a home or business street address -- it enables computers connected to the

Internet to properly route traffic to each other. The assignment of IP addresses to computers connected to the Internet is controlled by ISPs.

b. **Domain Name:** A domain name is a simple, easy-to-remember way for humans to identify computers on the Internet, using a series of characters (e.g., letters, numbers, or other characters) that correspond with a particular IP address. For example, “usdoj.gov” and “cnn.com” are domain names.

c. **Domain Name System:** The domain name system (“DNS”) is, among other things, a hierarchical convention for domain names. Domain names are composed of one or more parts, or “labels,” that are delimited by periods, such as “www.example.com.” The hierarchy of domains descends from right to left; each label to the left specifies a subdivision, or subdomain, of the domain on the right. The right-most label conveys the “top-level” domain. For example, the domain name “www.example.com” means that the computer assigned that name is in the “.com” top-level domain, the “example” second-level domain, and is the web server.

d. **Domain Name Servers:** DNS servers are computers connected to the Internet that convert, or resolve, domain names into Internet Protocol (“IP”) addresses. For each top-level domain (such as “.com”), there is a single company, called a “registry,” that determines which second-level domain resolves to which IP address. For example, the registry for the “.com” and “.net” top-level domains is VeriSign, Inc., which has its headquarters at 21355 Ridgetop Circle, Dulles, Virginia.

e. **Registrar & Registrant:** Domain names may be purchased through a registrar, which acts as the intermediary between the registry and the purchasers of the domain name. The individual or business that purchases, or registers, a domain name is called a “registrant.” Registrants control the IP address, and thus the computer, to which their domain name resolves. Thus, a registrant may easily move a domain name to another computer anywhere in the world. Typically a registrar will provide a registrant with the ability to change the IP address a particular IP address resolves through an online interface. Registrars typically maintain customer and billing information about the registrants who used their domain name registration services.

### **C. Relevant Companies**

12. Based upon information provided to me by GSK officials, I have learned that GSK is a global pharmaceutical corporation with tens of thousands of employees. GSK researches, develops, secures regulatory approval, manufactures, markets, and sells pharmaceutical products. GSK operates research facilities around the world, including one in Upper Merion, Pennsylvania.

13. “GoDaddy.com” is an internet domain registrar and web hosting company. As of December 2014, GoDaddy.com served approximately 13 million customers and had 4,908 employees worldwide. For a fee, GoDaddy.com creates and maintains business or personal webpages.

**C. Subjects of the Investigation**

14. YU XUE, a/k/a “Joyce.”

a. YU XUE worked as a research scientist for GSK from June 2006 until January 2016. She was a senior-level manager at GSK with oversight of 2 to 3 junior employees. Given her position, she had access to a wide array of GSK trade secret information. YU XUE worked at GSK’s research facility in Upper Merion, PA. As described below, YU XUE emailed GSK confidential trade secret information relating to a dozen or more products from her GSK e-mail account to her personal account and then forwarded that intellectual property to her conspirators and others. YU XUE also used her GSK computer to download a substantial amount of intellectual property from GSK’s network onto a thumb drive or other portable storage device to send this information to her conspirators. YU XUE founded RENOPHARMA along with her co-conspirators to market and sell the stolen intellectual property. YU XUE and her co-conspirators created, or caused to be created, the **SUBJECT ACCOUNT**.

b. YU XUE primarily worked to develop anti-cancer drugs using proteins to target receptor sites on cancer cells. These types of anti-cancer drugs generally typically cost pharmaceutical corporations more than \$1 billion and many years to develop before they can be turned into a commercially successful product. On June 20, 2006, YU XUE signed a Conditions of Employment Agreement with GSK. Pursuant to this agreement, YU XUE agreed that she would abide by GSK’s Company Code of Conduct. YU XUE agreed that she would “not engage in any activity in competition with or against the best interests of [GSK] and avoid all conflicts of interest with [GSK] or the appearance thereof.” YU XUE specifically agreed not to use any confidential GSK information for her own benefit or the benefit of other companies either during or after her term of employment. YU XUE agreed that all work she performed remained the “exclusive property” of GSK.

c. YU XUE is regarded as one of the top protein biochemists in the world. She has a Ph.D. in Biological chemistry from the University of North Carolina and an undergraduate degree from Peking University in China. According to her resume, she was the HER3 project co-leader at GSK working on monoclonal antibody design. She previously worked on structure modeling and antibody protein purification. According to her resume, she has successfully humanized and patented at least 4 separate antibodies. Prior to working at GSK, she worked for six years at the University of North Carolina as a research analyst.

15. TAO LI is one of the owners of RENOPHARMA, the corporations which were established to sell the stolen intellectual property. TAO LI and his co-conspirators created, or caused to be created, the **SUBJECT ACCOUNT**. YU XUE e-mailed some of the stolen intellectual property to TAO LI. TAO LI worked in China to sell the stolen intellectual property on behalf of RENOPHARMA. TAO LI’s role in the conspiracy included raising funds for RENOPHARMA from various sources. He has a B.S. in Biochemistry from Nankai University

in Tianjin, China, a M.S. in Molecular Biology from the Shanghai Institute of Biochemistry, and a Ph.D. in Molecular Biology from the University of North Carolina.

16. YAN MEI is another owner of RENOPHARMA. YAN MEI and his co-conspirators created, or caused to be created, the **SUBJECT ACCOUNT**. YU XUE e-mailed some of the stolen intellectual property to YAN MEI. YAN MEI worked in China to sell the stolen intellectual property on behalf of RENOPHARMA. YAN MEI also assisted YU XUE with the scientific processes for RENOPHARMA. His wife, LUCY XI, worked at GSK with YU XUE. YAN MEI received a B.S. in chemistry and molecular engineering from Peking University. He received his Ph.D. in Medicinal Chemistry from the University of Iowa in 2009.

17. TIAN XUE is the twin sister of YU XUE. TIAN XUE also worked for RENOPHARMA. According to an e-mail sent by YU XUE, YU XUE intended to hide all the proceeds of her criminal conduct in TIAN XUE's name. TIAN XUE also assisted YU XUE with some of the scientific processes for RENOPHARMA, processes which use the stolen GSK information and trade secret procedures. According to her resume, TIAN XUE has a B.S. in Biochemistry from Jilin University in Changchun, China, a M.S. in Biochemistry from Tsinghua University in Beijing, a Ph.D. in Immunology from the National Institute for Medical Research in London, and a M.S. in Computer Science and Information Technology from the University of North Carolina.

18. LUCY XI, a/k/a "Lu Xi," was the wife of YAN MEI. LUCY XI worked as a scientist at GSK from July 14, 2008 until November 3, 2015. While at GSK, LUCY XI e-mailed trade secret information from her GSK e-mail account to YAN MEI.

19. GONGDA XUE is the older brother of YU XUE. He works at the University of Basel in Switzerland. He previously worked at the Friedrich Miescher Institute for Biomedical Research which is part of the Novartis Research Foundation located in Switzerland. YU XUE e-mailed GONGDA XUE trade secret and otherwise confidential information to GONGDA XUE. In return, GONGDA XUE e-mailed YU XUE information which he labeled as "confidential" or "highly confidential".

20. Renopharma, Inc. was a corporation created by YU XUE and incorporated under the laws of the State of Delaware on July 16, 2012. Similar corporations called Shanghai Renopharma and Nanjing RenoPharma, Ltd. were created offshore, possibly in China. The evidence shows that the purpose of these corporations was to market and sell the stolen GSK information. RENOPHARMA advertised that it operated as a drug research and development company in China with limited U.S. affiliation. RENOPHARMA touted itself as "a leading new drug research and development company, specialized in providing products and services to support drug discovery programs at pharmaceutical and biotech companies. Our company is headquartered in Nan Jing, Jiang Su, P.R. China."

21. TAO LI described RENOPHARMA in an email in which he stated that he and two of his friends [YU XUE and YAN MEI] "are setting up a company [RENOPHARMA] and trying to find investors in China. One of my team members [YU XUE] has been working in a big pharmaceutical company [GSK] for years and is one of the best scientists in the world on

protein modeling, especially in antibody humanization and affinity maturation, which most pharmaceutical companies cannot do by themselves. Our plan is: First spend 1-3 years to set up a company in China and offer antibody humanization/affinity maturation services to companies worldwide, then spend another 3-4 years to develop our own antibody drugs.”

22. In another email, TAO LI further described RENOPHARMA, “The name of my company is Nanjing RenoPharma Inc. It’s located at Nanjing, a city in Eastern China, about 150 miles away from Shanghai. So far the company is running well. The major funding was from two private investors. We got some supports from the government, including some national awards and extra fundings, tax waive, and a free 4000 sqf lab space.”

23. In August 2015, a Chinese government news article identified TAO LI as having returned to China for a business start-up after having spent more than 10 years studying and working in the United States. The article, when translated into English, stated TAO LI “founded RENOPHARMA Inc. in Nanjing, which is focusing on research and development of antibody drug.” The article continues, quoting TAO LI as saying, “In these two years in China, governments in different levels have helped us a lot. This confirmed [to] us that the road we chose is right.” TAO LI further states in the article that, “he has received almost 2 million yuan [about \$300,000 depending on the volatile exchange rate] financial support from governments in different levels in Nanjing, Jiangsu province. Moreover, his company is enjoying many benefits like first two-year office area for free and bank loan convenience.”

24. On July 15, 2012, YU XUE emailed TAO LI and provided more information about RENOPHARMA and their respective roles in this venture. In particular, she stated, as translated from Mandarin Chinese:

I thought about the [company’s] operation method last night. [I believe] many years’ worth of experience and knowledge are the key [elements] for the company [RENOPHARMA]. Although I am not resigning from my position [at GSK] to go back [to China] at the initial stage, my time and energy spent is not going to be less than anyone else’s. As a matter of fact, it will only be more. The risk on the technology and the responsibilities are huge too. Simply using the reasons that I am not returning to China or I have little financial burden to decide not to give me wages doesn’t make any sense. If we operate with this methodology, then I will feel like an outsider, like a consultant, and not as a key member of the company. In order to promote motivation, the wage distribution should be that either no one gets paid or everyone gets paid equally. Everyone should give what they can. After reviewing the project proposal, the total for the wage is 1.2 million RMB, split evenly among all three high level managers, each one will get 400,000 RMB which is within your limit. I can leave my 400,000 RMB in the company for you to borrow if you don’t have enough funding. Please call me if you disagree.

#### **IV. THE INVESTIGATION**

##### **A. GSK Trade Secret Information**

25. YU XUE was involved in developing biopharmaceutical drugs for GSK. Many biopharmaceutical drugs are proteins which bind to receptor cells to cause the cell to act in a certain manner. Biopharmaceutical drugs can be very profitable, but they are also very expensive to research and develop and difficult to manufacture. Many of these drugs are developed to treat cancer or other serious ailments.

26. A concrete example is helpful to understand the business of biopharmaceutical drug research, development, and marketing. In the 1990's, another pharmaceutical company, Genentech, researched and developed an anti-cancer drug called Herceptin. In some forms of cancer, such as breast cancer, certain receptors on human cells which control growth and reproduction (called "HER2" receptors) may become "overexpressed." This means that a normal human cell might have, for example, 20,000 HER2 receptors, while a cancer cell might have 2 million HER2 receptors. Consequently, these cells reproduce uncontrollably forming a tumor. In layman's terms, Herceptin is a protein which binds with the HER2 receptor and shuts it off or slows it down, significantly impacting or slowing the cancer. Genentech spent a lot of money to research and develop Herceptin, but now they generate billions of dollars in revenue each year from selling Herceptin on the global market.

27. There are other receptors on cells which may impact other forms of cancer. One of the potential receptor sites is known as HER3. There are no current commercially available products which bind specifically to HER3. GSK and other pharmaceutical companies have been attempting for some time to develop a drug which binds to HER3 in a similar manner to the way that Herceptin binds to HER2. Correspondingly, GSK hopes to profit from the sale of such a drug in the same manner as Genentech did with Herceptin. YU XUE was one of the scientists at GSK working on this problem. Some of the items which YU XUE stole from GSK pertain to potential HER3 drugs. These potential drugs are often referred to in the scientific documents as "monoclonal antibodies" (mAb or moAb). Monoclonal antibodies are made by identical immune cells that are all clones of a unique parent cell (in contrast to polyclonal antibodies which are made from several different immune cells). One of the difficult challenges for pharmaceutical companies is to find an antibody which successfully "binds" to the target cell. A second difficult challenge is called humanization - which is the process of transforming an antibody which works well in animal experiments into an antibody which works well in humans. A third difficult challenge is in the manufacturing process - it is difficult to harvest the specific antibodies produced and purify the final product in order to safely inject it into the human body. The GSK information which YU XUE stole concerned all of these challenges. In addition, YU XUE stole information pertaining to other GSK products and products in development, even products she was not researching.

## **B. Summary of Investigation**

28. In summary, this investigation has revealed that YU XUE was part of a conspiracy that stole proprietary trade secret information primarily from GSK. YU XUE worked for GSK as a manager in research and development of these biopharmaceutical products. This stolen trade information essentially contained the blueprints and other research to reproduce biopharmaceutical products which GSK sells or intends to sell in the future and would greatly assist a competitor to manufacture the same or similar product in violation of GSK's intellectual

property rights. In furtherance of these efforts to profit from the sale of GSK proprietary information, YU XUE and her co-conspirators established RENOPHARMA (Renopharma, Inc. Shanghai Renopharma, Ltd., and Nanjing Renopharma, Ltd.) to facilitate the sale of the stolen trade secret information. They later created the **SUBJECT ACCOUNT** to help them market the stolen information.

29. YU XUE is assisted in these efforts by YAN MEI, TAO LI, LUCY XI, and TIAN XUE. YAN MEI and TAO LI attempted to market and sell the stolen GSK information to customers in China through RENOPHARMA. YU XUE, YAN MEI, and TAO LI also attempted to patent some drugs which GSK was developing ahead of GSK. LUCY XI was YAN MEI's wife and a former GSK employee. Based upon seized e-mails, this evidence reflects that LUCY XI also stole GSK information and provided it to YAN MEI. TIAN XUE was YU XUE's twin sister. TIAN XUE assisted YU XUE with some of the scientific work for RENOPHARMA. YU XUE instructed TAO LI and YAN MEI that her profits from RENOPHARMA be titled in TIAN XUE's name to hide her association with and participation in RENOPHARMA. In addition, YU XUE also e-mailed trade secret and otherwise confidential GSK information to her brother, GONGDA XUE.

30. Seized email records demonstrate that YU XUE transferred the stolen trade secret information via email from her GSK email account to her personal email account. From her personal email account, YU XUE then sent the proprietary trade secret information via email to other members of the conspiracy. In addition, information provided by GSK reflects that YU XUE downloaded over 350 files to an external data storage device on one day alone and downloaded many others during the time she worked at GSK. According to GSK, the files YU XUE downloaded contained powerpoint slides, business operation data, scientific research data, and other proprietary information. YU XUE downloaded this information to a thumb drive, external hard drive, or similar data storage device from her GSK computer in order to transport this information to her home computer or otherwise disseminate to her co-conspirators.

31. YU XUE and her co-conspirators acted with the apparent intention to profit from this highly valuable stolen information by selling it to GSK's business competitors in China. The stolen information would allow RENOPHARMA or another company to reproduce GSK's current and future pharmaceutical products without having to spend any funds on research and development. The information would also allow YU XUE, TAO LI, and YAN MEI to earn consulting fees from other pharmaceutical companies by using the information stolen from GSK. The information which YU XUE stole from GSK is potentially worth hundreds of millions of dollars or more. YU XUE stole more than a dozen specific products, even products she was not directly researching and developing.

32. According to GSK, the cost to develop one of these types of products which YU XUE stole frequently exceeds \$1 billion.

### **C. Search Warrants**

33. During the course of the FBI investigation, the FBI sought and obtained email communications between the targets of the investigation through a series of warrants to search

the targets' personal email accounts. On June 29, 2015, the Honorable Marilyn Heffley, United States Magistrate Judge for the Eastern District of Pennsylvania, signed a warrant to authorize the search of YU XUE's personal e-mail account (yxue2007@gmail.com). Google subsequently provided the FBI the account records pursuant to the search warrant which contained e-mails between XUE's personal e-mail account and various other co-conspirators, including YAN MEI, TAO LI, and TIAN XUE. These e-mail and internet messaging records showed that YU XUE forwarded some of the stolen proprietary GSK information to YAN MEI, TAO LI, and TIAN XUE with the apparent intention to resell this stolen information for pecuniary gain. YU XUE also forwarded some of the stolen trade secret information to her brother, GONGDA XUE, who was a scientist working in Switzerland.

34. In the same manner, on August 17, 2015, the Honorable Timothy R. Rice, United States Magistrate Judge for the Eastern District of Pennsylvania, signed warrants to authorize the search of four Google accounts belonging to YAN MEI (mylucyxl@gmail.com), TAO LI (taoli1973@gmail.com), YU XUE's husband, and TIAN XUE (xuetian2008@gmail.com). Google subsequently provided those records, primarily consisting of e-mails and internet messaging records. These records further showed YU XUE, TAO LI, YAN MEI, TIAN XUE, and LUCY XI transmitting GSK trade secret and otherwise confidential information amongst themselves and discussing the overall RENOPHARMA conspiracy.

35. On November 17 and November 19, 2015, the Honorable David R. Strawbridge, United States Magistrate Judge for the Eastern District of Pennsylvania, signed warrants to authorize the search of YU XUE's GSK office, YU XUE's GSK work computer, and LUCY XI's GSK work computer. Similar and corroborating evidence was obtained during these searches as was found by the FBI in previous searches.

#### **D. Specific Instances**

36. After obtaining through the search warrants the communications between the conspirators which included trade secret and otherwise confidential information, the FBI interviewed at least four different GSK scientists and showed them the seized e-mails. The GSK scientists identified 16 e-mails which YU XUE transmitted which contained trade secret information. Most of the trade secret information pertains to specific GSK manufacturing processes. Some of the trade secret information pertained to specific monoclonal antibodies developed by GSK. They identified numerous other documents which YU XUE sent which contained confidential, but not trade secret, information.

37. In addition, the FBI showed the seized e-mails to an expert witness retained by the government who was not associated with GSK (hereinafter "Expert 1"). Expert 1 has more than 35 years' experience in researching and developing biopharmaceutical products. He formerly worked as a Vice President for Bristol-Myers Squibb for Biologics Strategy and Biopharmaceutical Operations. He now operates a biopharmaceutical consulting company. He currently sits on the board of directors of ImmunoGen. As such, he is uniquely qualified to understand both the science and the business of biopharmaceuticals. Expert 1 reviewed the seized documents and also opined that they contained trade secret information.

38. The documents which contain trade secret information include:

a. On July 2, 2012, YU XUE (using yxue2007@gmail.com) e-mailed TAO LI (using taoli1973@gmail.com). Attached to the email is an internal GSK PowerPoint presentation titled "Anti-HER3 mAB" and identified a specific GSK antibody under development. The attachment was identified by GSK officials as containing both GSK trade secret information and other confidential, but not trade secret, information. The powerpoint contained GSK's strategy for developing an anti-HER3 monoclonal antibody and information on a specific candidate for anti-HER3 for clinical trials. The powerpoint outlined the development risks and opportunities of a specific anti-HER3 antibody candidate for GSK. The powerpoint opined that this candidate "would provide GSK with [a] package similar to Herceptin/HercepTest that showed great therapeutic value to cancer patients." It also provided the pre-clinical data in support of the candidate antibody and a thorough explanation of how it worked. The powerpoint also discussed the current status of other pharmaceutical corporations' anti-HER3 research and development, including Merrimack, Roche, ImmunoGen, and Amgen. The powerpoint opined that the GSK candidate "should represent [a] 'bio-better and bio-superior' system in comparison to existing competitors." The powerpoint further explained, "We can conclude . . . we can kill [the cancer] tumor [in a] different way that will complement each other to maximize the specific [cancer] cell killing." The powerpoint provided a draft clinical development strategy. According to GSK officials, this kind of sensitive trade secret information "would never be given out." [Document 35.]

b. On January 1, 2013, LUCY XI e-mailed her husband YAN MEI (using mylucyxl@gmail.com). The subject line of the e-mail read, "a good paper to read." In the body of the e-mail LUCY XI stated to YAN MEI, "You need to understand it very well. It will help you in your future business [RENOPHARMA]." Attached to the email is a GSK document titled, "Point to Consider in Determining Critical Quality Attributes for Therapeutic Monoclonal Antibodies." The attachment retained the GSK letterhead on each page. The attachment was identified by GSK officials as containing GSK trade secret information. The GSK document provided a current summary of GSK research into monoclonal antibodies. The document provided descriptions, schematic representations, and biological summaries of the antibodies which GSK used in its research and development projects. According to GSK officials, the document contained the business plan for GSK's quality control unit and constituted very sensitive information. [Document 33.]

c. On January 25, 2013, YU XUE (using yxue2007@gmail.com) e-mailed YAN MEI (using mylucyxl@gmail.com). Attached to the email were two documents. The first document is a powerpoint presentation titled, "Investigate fragmentation of aBCMA" written by YU XUE. The slides contained computer modeling of a specific GSK antibody. The second attachment contained another computer model. The first attachment was identified by GSK officials as containing GSK Trade Secret information. [Document 32.]

d. On April 11, 2013, YU XUE e-mailed a GSK report from her GSK account to her personal e-mail account (using yxue2007@gmail.com). The report detailed the design of experiment, validation, and platform method instruction and verification of analytical method for the quantitation of host cell proteins in monoclonal antibodies. The report described

in very specific detail GSK's procedures to test monoclonal antibodies. The report provided the list of reagents and assay solutions used by GSK scientists. The report then provided GSK's step-by-step instructions on how to perform these scientific tests. The report further provided GSK's validation procedures to determine if the product falls within the requisite standards. As such, GSK officials stated that the document contained GSK trade secret information relating to these processes. [Document 56.]

e. On September 25, 2013, YU XUE (using yxue2007@gmail.com) e-mailed TAO LI (using taoli1973@gmail.com) and YAN MEI (using mylucyxl@gmail.com) a GSK document. On January 9, 2014, YU XUE re-sent the same document to YAN MEI. Later that day, YAN MEI forwarded that document to TAO LI. The document is clearly identified as being GSK information and clearly marked "Confidential" on the top of each page. The document contained a GSK research report concerning GSK scientific research on specific monoclonal antibody candidates targeting the HER3 receptor. The document described in detail the "binding" capabilities and other important scientific characteristics of the antibody candidates. The report concluded that the scientific testing revealed that two specific candidates warranted further testing based upon the positive results achieved. Consequently, the GSK officials stated that this document contained highly sensitive trade secret information concerning GSK research into specific products in development. [Document 9.]

f. On November 8, 2013, YU XUE e-mailed a GSK powerpoint slide from her work e-mail account to GONGDA XUE's work e-mail account, who worked as a scientist in Switzerland. The powerpoint was authored by YU XUE. The front page of the powerpoint contained GSK's logo. The powerpoint is titled, "Structure, Computation, and Biopharmaceuticals." The powerpoint contained a summary of YU XUE's biopharmaceutical research for GSK. The powerpoint described GSK's procedures for developing and humanizing a monoclonal antibody. It contained models and descriptions of specific GSK antibody candidates targeting HER3 receptors. The powerpoint contained specific recommendations for GSK scientists working on these projects as well as hypotheses for future research. GSK officials stated that this document contained trade secret information as it pertained to specific products in development and specific GSK procedures. [Document Z.]

g. On November 28, 2013, YU XUE (using yxue2007@gmail.com) e-mailed a powerpoint presentation from her GSK e-mail account to her personal e-mail account. The presentation was titled "Antibody Drug(label) Conjugates Design" and indicated that it was authored by YU XUE. The presentation summarized YU XUE's scientific research for GSK, including computer modeling of specific antibodies. The powerpoint described GSK's specific procedures for producing and developing monoclonal antibodies, including step-by-step instructions. The document described the "final conjugation conditions" and an analytical results summary. GSK officials stated that the document contained GSK trade secret information. [Document B.]

h. On January 19, 2014, YU XUE (using yxue2007@gmail.com) e-mailed two GSK documents to TAO LI (using taoli1973@gmail.com). TAO LI then forwarded those documents on the same day to YAN MEI (using mylucyxl@gmail.com). Knowing that the document contained highly confidential GSK trade secret information, in the body of the e-mail,

YU XUE instructed TAO LI, “*Please do not spread. Thank you.*” The first document was a powerpoint presentation titled, “Anti TNF alpha BioBetter Program Introduction.” The powerpoint presentation included GSK research into ways to improve existing biopharmaceutical products by extending the half-life of monoclonal antibodies and extending dosing intervals. The document discussed the various diseases which these products could treat and opined that this development presented a “significant commercial opportunity” for GSK. The document referenced the fact that pharmaceutical corporations sold more than \$10 billion of these types of biopharmaceutical products each year. The document discussed the risks associated with the development of this kind of product and whether the development would interfere with other existing patents. The second document was a Word document summarizing the same proposal in written form. This document explained the objectives and the concept to improve the mechanism of action. It explained the target validation requirements for development. The document explained the potential benefits to patients on the improved pharmaceutical products. It also provided a manufacturing strategy and a projected sales forecast if such a product was developed. GSK officials explained that both of these documents contained GSK trade secret information. [Document 15.]

i. On February 17, 2014, YU XUE e-mailed a confidential GSK report from her GSK e-mail account to her personal e-mail account (yxue2007@gmail.com). Later that evening, YU XUE e-mailed the same document from her personal e-mail account (yxue2007@gmail.com) to YAN MEI (using mylucyxl@gmail.com). YAN MEI then forwarded the same document to TAO LI (using taoli1973@gmail.com) on the same date. The document was a quality control report on a specific GSK biopharmaceutical product. The bottom of each page was marked “confidential.” At the top of the first page, the document stated, “*If this template is used to provide information to external 3rd party, seek prior approval . . .*” The document described the specific GSK procedures for the construction of plasmids, which are used to grow monoclonal antibodies. The document contained the exact DNA sequence to build the plasmid. As such, GSK officials stated that this document contained confidential trade secret information. [Document GSK C.]

j. On March 3, 2014, YU XUE (using yxue2007@gmail.com) e-mailed GONGDA XUE a GSK powerpoint presentation titled, “An Introduction to Microbial & Cell Culture Development.” Each slide contained GSK’s logo. The document summarized GSK’s internal procedures for developing cell cultures used in biopharmaceutical research. The document showed how GSK structured its operations. The document contained diagrams of the machinery used by GSK to manufacture cell cultures. The document also discussed the specific types of cells which GSK used. One slide was titled, “Holy Grail of Cell Line Selection” – giving an indication of the importance of that information to GSK. The document discussed ways to improve cell environment to increase productivity. GSK officials stated that this document contained trade secret information relating to specific GSK scientific processes. [Document U.]

k. On March 3, 2014, YU XUE (using yxue2007@gmail.com) e-mailed GONGDA XUE a GSK powerpoint presentation training lecture titled, “An Introduction to Downstream Processing & Downstream Process Development (DPD).” The presentation described GSK’s purification procedures in manufacturing biopharmaceutical products. In order

to make a biopharmaceutical product, GSK grows the proteins (monoclonal antibodies) in huge vats, but these proteins must be purified before they can be injected into a patient. GSK's DPD department thus plays a crucial role in manufacturing biopharmaceutical products. In summarizing DPD's role in the manufacturing process, one slide quoted a GSK scientist as saying, "They give us something that looks like sewer sludge and we have to turn it into something that you are willing to inject into your veins." The powerpoint slide described precisely how GSK purified biopharmaceutical products, including diagrams and specific instructions. The powerpoint described the procedures GSK used to remove impurities and harvest the monoclonal antibodies from the "sewer sludge." The powerpoint identified the specific filtration process used by GSK. The powerpoint further described the procedures used by GSK to prevent viruses or other impurities from entering the final product. The powerpoint described the validation procedures used by GSK to ensure a high quality product that passed regulatory muster. Finally, the powerpoint provided GSK's material and operating costs for implementing these procedures and strategies for limiting those costs. GSK officials stated that this powerpoint slide contained GSK trade secret information regarding these specific processes. [Document W.]

1. On March 3, 2014, YU XUE (using yxue2007@gmail.com) e-mailed GONGDA XUE seven GSK documents. GSK officials stated that each of the following documents contained trade secret information. [Document X.]

(1) The first document was titled, "An Introduction to Downstream Process Development." This document contained almost exactly the same information as Document U described in the previous paragraph, although in an easier to read format.

(2) The second document was a powerpoint slide titled, "Overview of Small-scale Downstream Process Characterization for Late-phase Assets." This document further described GSK's commercial manufacturing processes and control strategy. In particular, the document described how GSK removed impurities during the manufacturing process and harvested the biopharmaceutical products. The document provided diagrams showing the exact materials GSK used to manufacture biopharmaceutical products. The document described the normal operating ranges and proven acceptable ranges for final GSK products.

(3) The third document was a GSK powerpoint slide entitled, "Lab Rotation Program." Each page of this presentation contained GSK's logo. The document described GSK's manufacturing operations activities. The document provided GSK's overall "vision and strategy" for manufacturing operations. The document described GSK's manufacturing capacity and equipment capabilities.

(4) The fourth document was a GSK powerpoint presentation entitled, "Virus Clearance Validation in DPD." The document described GSK's procedures to ensure that their end product was safe and did not contain any viruses. The document described the step-by-step details for GSK's procedures for purifying monoclonal antibodies. Finally, the document described GSK's costs for these quality control procedures and their regulatory responsibilities.

(5) The fifth document was a GSK powerpoint presentation titled “BioPharm Lab Rotation Program – Introduction to Preparative Chromatography & Process Development Fundamentals.” The powerpoint described GSK’s procedures for protein chromatography which GSK uses in the manufacturing process. The powerpoint described exactly how GSK’s chromatography machines were designed and configured. The powerpoint also described the particles used in GSK’s chromatography processes and the different types of chromatography used by GSK. The powerpoint also described GSK’s development sequences for new chromatography processes for monoclonal antibodies.

m. On February 3, 2015, YU XUE (using yxue2007@gmail.com) e-mailed a GSK document from her GSK e-mail account to her personal e-mail account. A few minutes later, YU XUE (using yxue2007@gmail.com) forwarded that same document to TAO LI (using taoli1973@gmail.com) and YAN MEI (using mylucyxl@gmail.com). The forwarding information on the e-mail revealed to TAO LI and YAN MEI that the document came from YU XUE’s GSK account. The document contained GSK’s specific procedures and instructions on how to filter a monoclonal antibody during the manufacturing process. GSK officials stated that this document contained trade secret information. [Document G.]

p. On August 17, 2015, YU XUE (using yxue2007@gmail.com) e-mailed a 17-page GSK report to TAO LI (using taoli1973@gmail.com) and YAN MEI (using mylucyxl@gmail.com). The report contained information on a specific product being developed by GSK for anti-cancer treatment. The report described the biology of the product and how it worked. GSK officials stated that this document contained GSK trade secret information. [Document 36/49.]

#### **E. January 5, 2016 Seizures**

39. On January 5, 2016, FBI agents arrested YU XUE and executed a search warrant at her home. During that search, FBI agents seized dozens of computers and electronic storage devices. These personal electronic devices contained a treasure trove of GSK confidential and trade secret information. According to her employment agreement, GSK expressly forbid YU XUE from maintaining GSK information on her personal electronic storage devices. GSK scientists and the government’s expert witness have identified at least seven separate documents which contained trade secret information. Based upon my training and experience and the evidence gathered during this investigation, I believe that YU XUE was hoarding GSK information to use on behalf of RENOPHARMA.

40. Also on January 5, 2016, FBI agents arrested TAO LI and seized numerous electronic devices in his possession incident to that arrest. The FBI subsequently sought and received a warrant to search those devices. TAO LI’s personal electronic devices also contained a treasure trove of GSK confidential and trade secret information. GSK scientists and the government’s expert witness have identified at least six separate documents which contained trade secret information. According to the metadata associated with those files, this information came from YU XUE’s GSK computer.

**F. Data Protection**

41. According to GSK officials, trade secrets are vital to pharmaceutical corporations such as GSK. GSK spends a lot of time and money developing pharmaceutical products and the processes to manufacture those drugs. GSK derives value from trade secret information by developing and selling pharmaceutical products. If their competitors received this information, GSK would be injured financially because their competitors would be able to develop the same or similar products to sell. Since their competitors did not incur the substantial development costs for the product, they would be able to sell the same product at a substantially lower price which would obviously impact GSK's revenues and profits. Consequently, GSK and other pharmaceutical companies protect this information and attempt to keep it secret by, inter alia, having their employees sign agreements restricting the use of this information. GSK and other pharmaceutical companies require their employees to be trained on handling and protecting confidential information. GSK and other pharmaceutical companies also use various computer programs in an attempt to prevent their employees from stealing data.

42. GSK officials indicated that all information generated within the company is considered GSK's proprietary information and belongs to GSK. GSK information must not be released externally unless it has been "Approved for External Release," to a third party under an appropriate confidentiality agreement, or a disclosure required by law. GSK's staff who receive, create, or handle GSK's proprietary information are responsible for categorization in accordance with the "Procedures for the Protection" of GSK's information. GSK's employees are forbidden from using proprietary information for other business or personal activities from which they, or others connected with them, might personally benefit. All GSK employees must ensure that electronic confidential information is only submitted or stored within applications, external web sites, electronic repositories, PCs, mobile devices or other IT systems that have restricted access to individuals based on a need to know basis and are managed by GSK or a third party that GSK has contracted with to process and manage the information.

43. GSK's policy on the acceptable use of IT indicates it is an unacceptable practice to store GSK's data on personal equipment such as home computers, external hard drives, PDAs or USB devices. Furthermore, forwarding, posting, or uploading GSK's confidential information to public e-mail accounts (e.g., Google, Yahoo) or any other external website not approved by GSK is forbidden.

44. Regarding YU XUE, the GSK officials stated that YU XUE did not have permission to transfer confidential information to third parties or external internet accounts, such as her personal e-mail account. The GSK officials stated that YU XUE would not be permitted to share GSK information without having prior authorization. GSK's representatives further indicated this authorization would only be granted after a panel of five entities within GSK collectively agreed that authorization should be granted. GSK also stated that it would be outside GSK policy to e-mail GSK information to a third party or a personal e-mail account.

45. All GSK employees are required upon acceptance of employment with GSK to read and acknowledge their understanding of GSK's Code of Conduct policy. The Code of Conduct policy is GSK's overarching policy which encompasses the protection of GSK's proprietary, trade secret information. Employees are required to read and sign the Code of Conduct policy on an annual basis. Each time an employee such as YU XUE or LUCY XI logged onto a GSK computer, they would be required to acknowledge a banner which read: "This computer system is the property of GlaxoSmithKline and is intended for operation by authorized users. You agree to comply with the company's established security and computer use policies and procedures and acknowledge that GlaxoSmithKline has discretion to monitor, use, record, or disclose any data or communications stored or transmitted on the system at any time."

46. Regarding LUCY XI, she worked as scientist for GSK in their Biopharmaceutical Analytical Sciences section from 2008 until she resigned that position on or about November 3, 2015 to take a position with another pharmaceutical company. LUCY XI was subject to the same conditions during her period of employment at GSK. LUCY XI did not have permission from GSK to transfer the GSK confidential information to third parties.

#### **G. Knowledge and Intent**

47. E-mails seized from these search warrants further established that the conspirators acted with the specific intent to steal GSK data and knew that the data obtained from GSK was stolen.

a. On April 1, 2012, YU XUE (using yxue2007@gmail.com) e-mailed a business plan for a new company called "Conjutech" to TIAN XUE (using xuetian2008@gmail.com). The plan was written in Chinese. It appears that this was the same general idea as RENOPHARMA with a different name. In the body of that e-mail, YU XUE wrote, "DO not give to her [unknown who "her" is] for now, you can have a look at it. It takes me a lot of time to finish it. Be very careful to send it out." On the same date, YU XUE (using yxue2007@gmail.com) e-mailed the same business plan to YAN MEI. YAN MEI sent a similar business plan to LUCY XI on March 21, 2012. Thus, both TIAN XUE and LUCY XI certainly knew what YU XUE intended to do. Furthermore, since LUCY XI signed a similar employment agreement with GSK which prohibited this kind of competition, based upon my training and experience and the evidence gathered during this investigation, I believe that LUCY XI certainly knew that YU XUE actions violated that agreement.

b. On June 20, 2012, YU XUE (using yxue2007@gmail.com) messaged with TAO LI (using taoli1973@gmail.com) about a draft RENOPHARMA document which they intended to use to market the stolen data at a pharmaceutical convention. YU XUE instructed TAO LI to delete a reference to "philadelphia PA" on the document. TAO LI asked, "why?" YU XUE replied, "A lot of people from GSK attend [sic]" the conference – demonstrating her concern that the stolen data might be traced back to her.

c. On June 28, 2012, TAO LI (using taoli1973@gmail.com) sent an e-mail to YUE XU (using yxue2007@gmail.com) which stated, "We 4 [TAO LI, YU XUE, YAN MEI,

and another person] may need [to] discuss together about the organization of the company [RENOPHARMA] . . . . You [YU XUE] are the core person in this project and you need to think about how to protect yourself.” In other words, TAO LI wanted to discuss with his conspirators how they were going to protect themselves from being apprehended by law enforcement.

d. On July 8, 2012, YU XUE (using yxue2007@gmail.com) e-mailed the RENOPHARMA business plan to TIAN XUE (using xuetian2008@gmail.com). While written in Chinese, the cover page stated that RENOPHARMA would be providing monoclonal antibody humanization services. TIAN XUE knew that she was not an expert in monoclonal antibody humanization, therefore, the services obviously would be provided by YU XUE who was an expert in that field.

e. On July 2, 2012, YU XUE (using yxue2007@gmail.com) messaged with TAO LI (using taoli1973@gmail.com) and stated that she would send HER and EGFR “stuff” from her “personal computer”. TAO LI replied, “OK.” YU XUE stated that it was too dangerous to send this data from “the company” [GSK]. TAO LI replied, “yeah, we should be very careful.” Thus, based upon my training and experience and the evidence gathered during this investigation, I believe YU XUE intended to send proprietary GSK research data relating to HER or EGFR receptors from her home computer, rather than her office computer, because she was concerned that she might get caught stealing this data from GSK. Acknowledging their criminal conduct and the conspiracy, TAO LI agreed.

f. On July 3, 2012, YU XUE (using yxue2007@gmail.com) messaged with TAO LI (using taoli1973@gmail.com). TAO LI asked YU XUE if she had time to talk on the phone. YU XUE replied that she did. TAO LI asked YU XUE, “is it ok to call your office? People around you?” YU XUE replied that it was acceptable for her to talk because she had her “own office.” YU XUE then stated, “*hopefully nobody listen the phone* [sic].” Thus, based upon my training and experience and the evidence gathered during this investigation, I believe TAO LI and YU XUE intended to discuss details of the conspiracy to steal proprietary information from GSK during this phone conversation. At the time of this message exchange, YU XUE was sitting in her office at GSK. TAO LI wanted to ensure that there were no other Chinese-speaking GSK employees around to ensure that they would not be caught discussing the details of their conspiracy to steal proprietary information from GSK. YU XUE indicated that her office was a private place to talk because there were no other Chinese speakers around, but expressed concern that her phone might be wiretapped, again, demonstrating her knowledge that her conduct was criminal.

g. On July 31, 2012, YAN MEI (using mylucyxl@gmail.com) messaged with LUCY XI about YU XUE’s future plans. LUCY XI told YAN MEI that YU XUE intended to quit her job at GSK in one or two years. LUCY XI explained that YU XUE wanted to “*get the money first*.” YAN MEI replied, “that is our plan” – meaning that once the stolen GSK data is resold, all of the conspirators will have enough money to quit their jobs. LUCY XI replied, “I think it is reasonable to do that” and “that is a good solution.” LUCY XI then stated cryptically, “Dont offer details until they check for Yue’s [YU XUE] status.”

h. Later that afternoon, YAN MEI (using mylucyxl@gmail.com) and LUCY XI exchanged more messages. YAN MEI explained to LUCY XI that he had almost completed the “R&D plan” and “CRO plan” for RENOPHARMA. LUCY XI suggested that YAN MEI “check some books of negotiation and leadership” in order to build up his skill set for his job at RENOPHARMA. LUCY XI commented, “You need to build up those [sic] skills.” LUCY XI then suggested that YAN MEI “be humble and receptive” at RENOPHARMA business meetings and “Don’t assume you are naturally good.” LUCY XI related, “Some people are naturally better than others in negotiation, building relationship [sic] and leadership, but everyone has room to grow and improve”.

i. On August 28, 2012, YAN MEI (using mylucyxl@gmail.com) messaged with LUCY XI about YU XUE. LUCY XI complained to YAN MEI that YU XUE had been “annoying” her recently. YAN MEI counseled LUCY XI, “don’t lose [your] temper” with YU XUE. LUCY XI replied, “I won’t . . . *she is the queen.*” At the end of the conversation, LUCY XI stated, “Yu [YU XUE] showed me an email she drafted.” Discussing the terms of a RENOPHARMA deal, LUCY XI suggested, “I think you should take out the 10% to 25% out. It is too much. let’s just use 30% as the starting point.” Based upon my training and experience and the evidence gathered during this investigation, I believe that this e-mail demonstrates YAN MEI and LUCY XI’s knowledge that YU XUE was the critical piece of the conspiracy to steal information from GSK and jointly profit from it and were willing to tolerate her idiosyncrasies. Moreover, the e-mail further shows LUCY XI’s participating in the fraud conspiracy by reviewing YU XUE’s work and making suggestions regarding business operations.

j. On September 4, 2012, LUCY XI continued to press YAN MEI (using mylucyxl@gmail.com) about his RENOPHARMA work. Apparently, both YAN MEI and TAO LI were working on a presentation. LUCY XI instructed YAN MEI, “You need to practice before you present.” LUCY XI then stated, “I told Yu [YU XUE] that you did not send [a] copy [of the presentation] to her because Tao [TAO LI] wants to combine yours with his and then Tao [TAO LI] will send it to Yu [YU XUE].” LUCY XI chastised YAN MEI, “Be careful in the future. Don’t disappoint me anymore. it is really stupid the way you handle stuff.”

k. On October 11, 2012, YU XUE (using yxue2007@gmail.com) e-mailed YAN MEI (using mylucyxl@gmail.com) a RENOPHARMA powerpoint presentation titled, “Structure guided design of antibodies for therapeutic application.” The powerpoint presentation discussed how RENOPHARMA would engineer the next generation of antibodies. The presentation discussed RENOPHARMA’s expertise in humanization, affinity maturation, and manufacturing – all the work YU XUE performed for GSK. The presentation showed computer generated models of potential antibody candidates and how they would bind to the receptors.

l. On October 11, 2012, YU XUE (using yxue2007@gmail.com) messaged TAO LI (using taoli1973@gmail.com) and stated, “I suggest do not send any email to them. we can TC [teleconference] but do not send them.” Based upon my training and experience and the evidence gathered during this investigation, I believe that YU XUE did not want TAO LI to forward a trade secret or confidential GSK presentation to someone outside of RENOPHARMA. YU XUE suggested that they have a teleconference instead. A few minutes later, TAO LI messaged with YU XUE about the same presentation. YU XUE indicated that she was not

“comfortable” sending the stolen file to another company in China. YU XUE instructed TAO LI, “do not give any slide copy to them” because it was “too dangerous.” Thus, I further believe YU XUE was reluctant to turn over the stolen GSK powerpoint presentation to a third party for fear that she might get caught.

m. On November 26, 2012, YAN MEI (using mylucyxl@gmail.com) e-mailed TAO LI (using taoli1973@gmail.com) and YU XUE a published research paper titled, “Advances in Targeting HER3 as an Anticancer Therapy.” The paper was published on October 10, 2012. TAO LI responded that he did not see “the one developed by GSK” in the published paper. TAO LI continued, “It seems risky to work on anti-HER3 only. Good thing is that not many companies are working on this. Any comments Yu?”

n. On January 15, 2013, TAO LI (using taoli1973@gmail.com) messaged with YU XUE (using yxue2007@gmail.com). YU XUE told TAO LI that she “got in detailed information [presumably from GSK] about how to sequence mouse antibody in hybridoma cells.” YU XUE told TAO LI that she would send him that information from her “home computer tonight.” TAO LI instructed YU XUE, “Let me get it next time I visit you. *Don’t forward using e-mails.*” Based upon my training and experience and the evidence gathered during this investigation, I believe that TAO LI cautioned YU XUE not to send the trade secret information by e-mail and stated that he would pick up that information in person to prevent them from getting caught sending the stolen GSK data.

o. On April 2, 2013, TAO LI (using taoli1973@gmail.com) sent an e-mail to YAN MEI (using mylucyxl@gmail.com) about a researcher in Wisconsin who was charged with stealing details of a cancer-fighting compound. YAN MEI replied, “*This sounds scary.*” Based upon my training and experience and the evidence gathered during this investigation, I believe that TAO LI sent the e-mail as a warning to his conspirators that they needed to be careful stealing GSK data to prevent themselves from being caught.

p. On October 11, 2013, LUCY XI sent YAN MEI (using mylucyxl@gmail.com) an e-mail from her GSK account. In the e-mail LUCY XI forwarded an e-mail she had received from another GSK employee attaching a newspaper article regarding two scientists working at Eli Lilly who had been indicted for stealing trade secrets.

q. On October 11, 2013, YU XUE (using yxue2007@gmail.com) sent TAO LI (using taoli1973@gmail.com) and YAN MEI (using mylucyxl@gmail.com) an e-mail with a link to a newspaper article about an Eli Lilly scientist indicted for stealing trade secrets. Based upon my training and experience and the evidence gathered during this investigation, I believe that YU XUE sent the e-mail as a warning to her conspirators that they needed to be careful stealing GSK data to prevent themselves from being caught. In a subsequent exchange of messages later that day, YU XUE warned TAO LI that “all GSK [employees] had a meeting this morning – presumably to discuss data protection in light of the Eli Lilly case. YU XUE stated that GSK set up a “hotline” – presumably for GSK employees to report data breaches. YU XUE then commented “*so scary*” demonstrating her fear of being caught for stealing GSK proprietary data. YU XUE then instructed TAO LI, “Please do not send any DOc contained [sic] GSK data out” and “DO not mention Her3 [human receptor research].”

r. On October 23, 2013, a person e-mailed TAO LI's wife and stated, "When you get a chance can you please ask your husband for information or a confidentiality agreement for his biochemical company. I want to test the levels of a naturally occurring item in certain products before and after the manufacturing/processing process." On October 25, 2013, TAO LI's wife attached a confidentiality agreement and replied, "I asked my husband Tao. He said his company can offer the service." On November 16, 2013, the e-mail chain was forwarded to TAO LI showing that TAO LI certainly understood the importance of a confidentiality agreement.

s. On October 27, 2014, YU XUE (using yxue2007@gmail.com) exchanged e-mails with GONGDA XUE. GONGDA XUE asked, "I have a question for you and the company in china: who is the real and practical owner? I mean the person who has the absolute control of this company? Do you have shares sorted out?" YU XUE replied that the owners were "Myself, Litao [TAO LI] and Meiyao [YAN MEI]. We three make up the company [and] are owner[s]. I have the absolute control of company. If we have really good data in the near future, I will quit the job in GSK right away. My stocks is occupied by taoli [TAO LI] for now, but we have law document notarized. I have the highest stock share which is 30%, taoli [TAO LI] and yanmei [YAN MEI] each has 21% share, the reset of share for the people invest money and also some left over for the future key people [who] join the company."

t. GONGDA XUE replied to the previous e-mail with a different proposal. He noted that he held the patent on an antibody and stated "I have planned for making up a company for some time." GONGDA XUE suggested that YU XUE form another company with him. GONGDA XUE suggested that they "co-patent" the antibodies that YU XUE was currently working on. He noted that he had financial "resources" he could invest in the company and connections with a research technology fund in Switzerland for additional investment funds. GONGDA XUE then began to criticize YU XUE's contract with RENOPHARMA. He opined that YU XUE's 30% share in the company was too low and that if TAO LI (21%) and YAN MEI (21%) joined forces, they would control a larger share of RENOPHARMA. GONGDA XUE told YU XUE that she should control "more than 50%" of the company. GONGDA XUE told YU XUE that she "should NOT quit" her job because many "startups die after one or two years." Based upon my training and experience and the evidence gathered during this investigation, I believe that GONGDA XUE may have been trying to get YU XUE to form a company with him so that he could profit from either YU XUE's expertise or the stolen GSK information.

u. On May 4, 2012, TIAN XUE (using xuetian2008@gmail.com) messaged with YU XUE (using yxue2007@gmail.com). TIAN XUE asked, "how is your presentation?" YU XUE replied, "It is very good." YU XUE asked if TIAN XUE received the "business plan" and commented "your name is there." TIAN XUE replied, "Yes I got it and read it." YU XUE asked, "Are you ok with your discription [sic]?" TIAN XUE replied, "[Yes,] very much." Concerned for their safety and knowing what they were doing was illegal, TIAN XUE asked, "is ok you sent this plan from your company email?" YU XUE assured her, "it is ok."

## **H. The SUBJECT ACCOUNT**

48. As recently as February 2017, the **renopharma.com** website stated, "Welcome to Renopharma Inc. Ltd". The **SUBJECT ACCOUNT** further stated, "We are a leading new drug research and development company, specialized in providing products and services to support drug discovery programs at pharmaceutical and biotech companies. Our company is headquartered in Nan Jing, Jiang Su, P.R. China." The **SUBJECT ACCOUNT** further offered services such as monoclonal antibody development, critical quality attributes analysis, and peptide synthesis and modifications. As described above, these services are based, in whole or in part, on information stolen from GSK. The **SUBJECT ACCOUNT** provided a point of contact as YAN MEI at yanmei@renopharma.com.

49. A search of publicly available WHOIS domain name registration records revealed that the **renopharma.com** domain was registered on or about June 15, 2012 through the registrar VeriSign, Inc., which has its headquarters at 21355 Ridgetop Circle, Dulles, Virginia. The publicly available WHOIS database lists the registrant of the **renopharma.com** domain as YU XUE.

50. In May 2017, GoDaddy.com, LLC disabled the **SUBJECT ACCOUNT** for a period of 90 days pending the application of this seizure warrant.

51. Based on the review of the RENOPHARMA documents seized in this investigation and the above information, RENOPHARMA's business is selling the confidential and trade secret information stolen from GSK. The **SUBJECT ACCOUNT** is used to advertise RENOPHARMA's sale of the confidential and trade secret information stolen from GSK.

## **V. PERTINENT STATUTES**

### **A. Offense Conduct**

52. Title 18, United States Code, Section 1832 provides:

(a) Whoever, with intent to convert a trade secret, that is related to a product or service used in or intended for use in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly--

(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information;

(2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates,

transmits, delivers, sends, mails, communicates, or conveys such information;

(3) receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;

(4) attempts to commit any offense described in paragraphs (1) through (3); or

(5) conspires with one or more other persons to commit any offense described in paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy,

shall, except as provided in subsection (b), be fined under this title or imprisoned not more than 10 years, or both.

53. Title 18, United States Code, Section 1839(3) defines the term “trade secret” as:

(3) the term “trade secret” means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if --

(A) the owner thereof has taken reasonable measures to keep such information secret; and

(B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public.

**B. Forfeiture**

54. Title 18, Section 1834, applies criminal forfeiture to trade secret violations and provides:

Forfeiture, destruction, and restitution relating to this chapter shall be subject to section 2323, to the extent provided in that section, in addition to any other similar remedies provided by law.

55. Title 18, Section 2323 provides:

(a) Civil Forfeiture.

(1) Property subject to forfeiture. The following property is subject to forfeiture to the United States Government:

(A) Any article, the making or trafficking of which is, prohibited under section 506 of title 17, or section 2318, 2319, 2319A, 2319B, or 2320, or chapter 90, of this title.

(B) Any property used, or intended to be used, in any manner or part to commit or facilitate the commission of an offense referred to in subparagraph (A).

(C) Any property constituting or derived from any proceeds obtained directly or indirectly as a result of the commission of an offense referred to in subparagraph (A).

(2) Procedures.

The provisions of chapter 46 relating to civil forfeitures shall extend to any seizure or civil forfeiture under this section. For seizures made under this section, the court shall enter an appropriate protective order with respect to discovery and use of any records or information that has been seized. The protective order shall provide for appropriate procedures to ensure that confidential, private, proprietary, or privileged information contained in such records is not improperly disclosed or used. At the conclusion of the forfeiture proceedings, unless otherwise requested by an agency of the United States, the court shall order that any property forfeited under paragraph (1) be destroyed, or otherwise disposed of according to law.

(b) Criminal Forfeiture.

(1) Property subject to forfeiture.

The court, in imposing sentence on a person convicted of an offense under section 506 of title 17, or section 2318, 2319, 2319A, 2319B, or 2320, or chapter 90, of this title, shall order, in addition to any other sentence imposed, that the person forfeit to the United States Government any property subject to forfeiture under subsection (a) for that offense.

(2) Procedures.

(A) In general. The forfeiture of property under paragraph (1), including any seizure and disposition of the property and any related judicial or administrative proceeding, shall be governed by the procedures set forth in section 413 of the Comprehensive Drug Abuse

Prevention and Control Act of 1970 (21 U.S.C. 853), other than subsection (d) of that section.

(B) Destruction. At the conclusion of the forfeiture proceedings, the court, unless otherwise requested by an agency of the United States shall order that any—

(i) forfeited article or component of an article bearing or consisting of a counterfeit mark be destroyed or otherwise disposed of according to law; and

(ii) infringing items or other property described in subsection (a)(1)(A) and forfeited under paragraph (1) of this subsection be destroyed or otherwise disposed of according to law.

(c) Restitution.

When a person is convicted of an offense under section 506 of title 17 or section 2318, 2319, 2319A, 2319B, or 2320, or chapter 90, of this title, the court, pursuant to sections 3556, 3663A, and 3664 of this title, shall order the person to pay restitution to any victim of the offense as an offense against property referred to in section 3663A(c)(1)(A)(ii) of this title.

56. Title 18, United States Code, Section 981(b)(2) provides, in pertinent part:

Seizures pursuant to this section shall be made pursuant to a warrant obtained in the same manner as provided for a search warrant under the Federal Rules of Criminal Procedure.

Title 18, United States Code, Section 981(b)(3) provides, in pertinent part:

A seizure warrant may be issued pursuant to this subsection by a judicial officer in any district in which a forfeiture action against the property may be filed under section 1355(b) of Title 28.

Title 28, United States Code, Section 1355 provides, in pertinent part:

A forfeiture action or proceeding may be brought in (A) the district court for the district in which any of the acts or omissions giving rise to the forfeiture occurred.

57. Title 21, United States Code, Section 853(f) provides, in pertinent part:

(f) Warrant of seizure. The Government may request the issuance of a warrant authorizing the seizure of property subject to forfeiture under this section in the same manner as provided for a search warrant. If the court determines that there is probable cause to believe that the property to be

seized would, in the event of conviction, be subject to forfeiture and that an order under subsection (e) of this section may not be sufficient to assure the availability of the property for forfeiture, the court shall issue a warrant authorizing the seizure of such property.

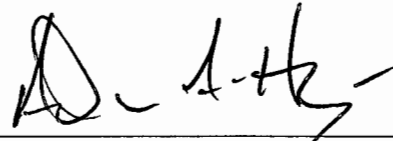
Title 21, United States Code, Section 853(1) provides:

The district courts of the United States shall have jurisdiction to enter orders as provided in this section without regard to the location of any property which may be subject to forfeiture under this section or which has been ordered forfeited under this section.

**V. CONCLUSION**

58. Based on the above facts, the **SUBJECT ACCOUNT** is property used or intended to be used to commit or facilitate the commission of violations of Title 18, United States Code, Section 1832 (theft of trade secrets). Accordingly, the **SUBJECT ACCOUNT** is subject to seizure and forfeiture to the United States under Title 18, United States Code, Sections 981(b), 1834 and 2323, and Title 21, United States Code, Section 853(f).

59. Neither a restraining order nor an injunction is sufficient to guarantee the availability of the **SUBJECT ACCOUNT** for forfeiture. By seizing the **SUBJECT ACCOUNT** and redirecting it to another website, the Government will prevent third parties from acquiring the name and using it to commit additional crimes. Furthermore, seizure of the **SUBJECT ACCOUNT** will prevent third parties from continuing to access the renopharma.com website.



ANDREW HAUGEN  
Special Agent  
Federal Bureau of Investigation

Sworn and subscribed  
before me this 19<sup>th</sup> day  
of September 2017.



HONORABLE LYNNE A. SITARSKI  
United States Magistrate Judge

## ATTACHMENT A

### **I. Seizure Procedure**

A. The seizure warrant will be presented in person or transmitted via facsimile or email to personnel of the domain name registry listed in Section II ("Subject Registry") and the domain name registrars listed in Section III ("Subject Registrars") who will be directed, for the domain names listed in Section IV ("Subject Domain Names") for which it serves as the top-level domain registry, to make any changes necessary to restrain and lock the domain name pending transfer of all rights, title, and interest in the Subject Domain Name to the United States upon completion of forfeiture proceedings.

B. Upon seizure of the Subject Domain Names, the Subject Registry shall point the Subject Domain Names to renopharmaseized.com, at which the Government will display a web page with the following notice:

*This domain name has been seized by the Federal Bureau of Investigation pursuant to a seizure warrant issued by a United States District Court under the authority of 18 U.S.C. §§ 981, 1834, and 2323.*

*Theft of trade secrets is a federal crime that carries penalties of up to ten years in federal prison, a \$250,000 fine, forfeiture, and restitution (18 U.S.C § 1832).*

C. Upon seizure of the Subject Domain Names, the Subject Registry shall take all steps necessary to restrain and lock the domain at the registry level to ensure that changes to the subject domain names cannot be made absent a court order or, if forfeited to the United States government, without prior consultation with the Federal Bureau of Investigation. The DNS record should be altered to remove any applicable name servers.

D. Upon seizure of the Subject Domain Names, the Subject Registrars shall modify any records, databases, tables, or documents that are used by the Subject Registrars to identify the owner of the Subject Domain Names to reflect the seizure of the Subject Domain Names. These changes relate to the following records, if they exist:

1. The "Technical Contact" and "Administrative Contact" fields will reflect the following information:
  - a) Name: Federal Bureau of Investigation
  - b) Address: 600 Arch Street, 8<sup>th</sup> Floor  
Philadelphia, PA 19106
  - c) Country: USA
  - d) Telephone: 215-418-4000
  - e) Email: aahaugen@fbi.gov
  - f) Fax: 215-418-4487

2. Any remaining fields will be changed so they do not reflect any individual or entity.

E. The Subject Registry shall take any steps required to propagate the changes detailed in Section D to any applicable DNS servers.

**II. Subject Registry**

Verisign, Inc.  
21355 Ridgetop Circle  
Dulles, Virginia 20166

**III. Subject Registrars**

Yu Xue  
31 Knickerbocker Lane  
Malvern, PA 19355

c/o Peter Zeidenberg, Esq.  
Arent Fox LLP | Attorneys at Law  
1717 K Street, NW  
Washington, DC 20006-5344

**IV. Subject Domain Names**

**renopharma.com**